

Next-Generation Advanced Security systems for Communities Using Integrated IoT and Blockchain Over Cloud Computing

Aadam Quraishi¹, Maher Ali Rusho², Faisal Yousef Alghayadh³, V. Mahalakshmi⁴, Mukesh Soni⁵, and Mohammed Wasim Bhatt^{6,*}

¹M.D. Research, Intervention Treatment Institute, Houston Texas, USA

²Department of Lockheed Martin Engineering Management, University of Colorado, Boulder, Colorado

³Computer Science and Information Systems Department, College of Applied Sciences, AlMaarefa University, Riyadh, Saudi Arabia

⁴Department of Computer Science, College of Engineering and computer science, Jazan University, Jazan 45142, Saudi Arabia

⁵Dr. D. Y. Patil Vidyapeeth, Pune, Dr. D. Y. Patil School of Science & Technology, Tathawade, Pune, India

⁶Model Institute of Engineering and Technology, Jammu, J&K, India

Abstract

According to human requirements, various structures are being constructed and require some protection from fire accidents, floods, earthquakes, any gas leaks, and any other concerns that may arise in the neighborhood. So far, their security goal is to propose a system integrated with blockchain and an IoT system. We structure the system in different steps in our proposal to process the alarm rung by IoT devices. This IoT gadget may be used in either a private or public setting. To do this, we must process the various settings for checking and responding to the devices. Data centers that interact between sender and recipient will verify blockchain data. Finally, we provide a security solution to avoid reply assaults, transmission interruptions, and data integrity. This entire system may work together to promote community safety and eliminate avoidable disputes.

Keywords

Blockchain, Internet of Things, Cloud Computing, Community Safety, Data encryption.

1. Introduction

IoT is one of the best technologies that will integrate many components. IoT can gather data from the existing parts; each member may unique IoT have the ability to transfer the data to the cloud. Various incidents have happened in the system; using a standard IoT system was to make attention to the incident. IoT systems ensure the safety of the network with the different components connected to the system [1]. IoT will include various techniques, step-by-step processes and actions/reactions that concentrate on increasing safety by using IoT [2].

IoT security refers method to be used by internet-connected devices. IoT is a very vast technology; in our work, it becomes broader. IoT security is used to protect the private/ public community. By using IoT technology, there is 30-35% growth in every field [3].

IoT will collect data in real-time, which will be used to make a decision. It may be accurate/predicted. The IoT can also understand the security strategies to protect the corresponding field [4].

Proceedings of SNSFAIT 2024: International Symposium on Securing Next-Generation Systems using Future Artificial Intelligence Technologies, Delhi, India, August 08-09th, 2024

* Corresponding author : wasimmohammad71@gmail.com (M.W. Bhatt)

† These authors contributed equally.

✉ aadamquraishi@yahoo.com (A. Quraishi); maher.rusho@colorado.edu (M.A. Rusho); basavadeepthihm@gmail.com (F.Y. Alghayadh); mlakshmi@jazanu.edu.sa (V. Mahalakshmi); mukesh.research24@gmail.com (M. Soni); wasimmohammad71@gmail.com (M.W. Bhatt)



© 2024 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

Blockchain technology is one of the easy to decentralize and distribute the record with digital assistance without proper acceptance/approval; nobody can change the data from the records [5]. A blockchain stores the data in the blocks of data chains. By using the appropriate acceptance/approval by the admin/ digital program, data cannot be modified/deleted/transferred [6]. The blockchain maintains the proper transparency between the admin and the public; The clarity will increase the trust now blockchain is one of the prime technologies in safety part [7].

2. Methodology

This research work proposes a methodology by integrating the IoT and blockchain technology for community safety and security purpose. In proposed method have a different practice. Figure 1 shows the methodology by integrating the IoT and blockchain technology for community safety and security purpose for smart cities.

Blockchain centers

Blockchain centers receive the information from IoT related devices and store/record the received data in the different device nodes [8]. This recorded/stored data can monitor by the community member who wants to verify the recorded/ stored data by the blockchain centers. They can view by security guards.

Community

Community members may belong to residential, commercial and mixed according to the type of community needed to install the IoT device and security guard.

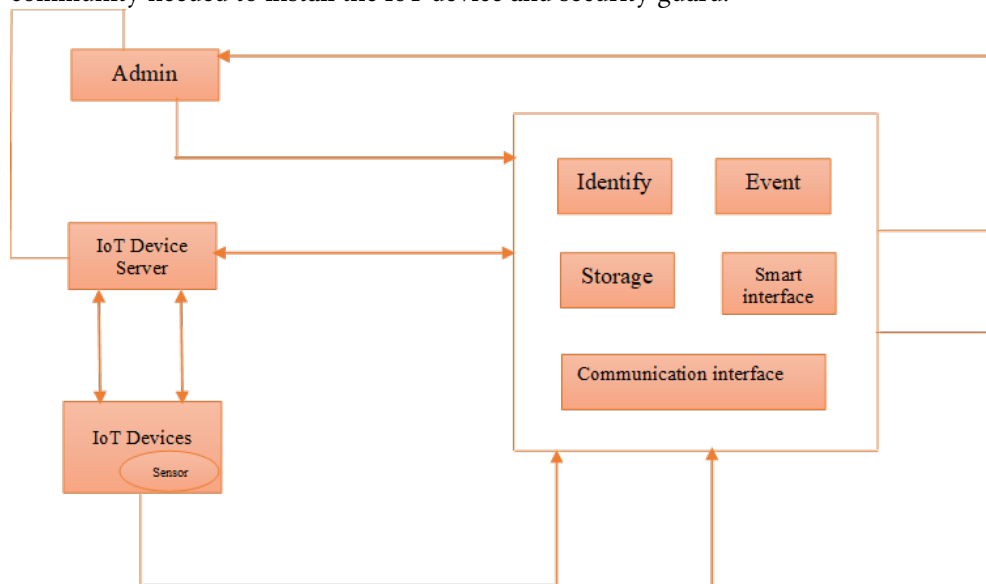


Figure 1. Methodology by integrating the IoT and blockchain technology for community safety and security purpose

Occupants

All the occupants living in the community have an option to install the IoT device in the private domain because they need the safety of their belongings [9]. If they are installed IoT devices, they should have mobile with the application. This application requires login through the blockchain centers. Using their login, we monitor all private domains by IoT devices.

Security guard

The security guard will work under the admin. The security guard should mentor the committee at all times. If any unknown or dangerous event occurs, the security guard should react immediately to save the community or community members [10].

Supervisor

Supervisor appointed by community management. The Supervisor should manage all the security guards. The Supervisor will give all types of permissions to the security guard to monitor community safety [11].

IoT Devices

IoT devices are cameras and sensors.

Cameras: Cameras take the images of the community. Cameras are fitted in the community, public or private domains [12]. Cameras are installed in public and private realms but need to determine how many cameras must be installed.

Sensors:

Sensors can find a dangerous moment like smoke detection, pathfinder, emergency button and other devices to identify the hazardous moment [13].

Log service:

Every camera recorded video is saved in a log server, and the server may use a physical component or cloud-based server [14]. The log server needs to read all the recorders.

2.1. Process flow of the proposed methodology

Step1: Every community member needs to require the IoT device through proper technology.

Step2: The IoT device records/monitors every unsymmetric event and send the information to the security guard and registered community members.

Step 3: The security guard will check the received event information through the IoT based Surveillance system.

Step 4: After verification, the security guard will solve the problem/ received issue, update the log server, and mark it as information in the blockchain centre.

Step 5: If the IoT device is relevant to the private community, the alarm will ring/ information will pass to the appropriate community member via the installed application.

Step 6: The community member will verify the situation via the application and update the same event information to the blockchain centers.

Step 7: The community member will need a security guard to help them. He can have an option to choose.

2.2. Installation of application

In the particular installation of the application, In the device is major concerned with the blockchain center to initiate the mutual communication to the community. All the community members need to register their data with the application in online mode with the application. The blockchain center will add the registered community member through his application with a registered address and broad cast with the community as a hash-aundro-DSDV routing scheme. The community area will connect with the blockchain center of a concerned security guard. Before passing the information, an authentication process should verify the received/ sender information verified by the registered address [15]. The device/ system should match the address respectively. Figure 2 below shows the algorithm for install the application.

Algorithm for installation of application:




1. Generate the registration link through the blockchain centers.
2. Forward the registration link  Through proper channel
3. Receives the registration link through blockchain centers.
4. For($i=0; i=n-1; i++$)
5. Check block chain center
6. If
7. Registration link \in block chain center
8. Then
9. Register the aundro address in the mobile
10. Else
11. Deeney the registration request
12. End if
13. Broadcast the registered aundro address in the blockchain centers.
14. Share the information blockchain centers  security guard  Community member
15. Return: list out the registered community member and MAC/ Aundro address.

Figure 2. Algorithm for install the application

2.3. Authentication phase

Figure 3 represents the step-by-step process for authentication for a registered community member. This entire phase will work under the community to the blockchain. IoT devices are interconnected in the whole system to exchange the data inside the design only [16]. For that purpose, authentication is needed to exchange the data in the system for security purposes. Every data/ message is assigned the ID and aundro address for that authentication [17]. This information is verified by the blockchain centers and matched with the ID and address of the registered community member. Then, only data will transfer authentically if any data/information is needed from the community member [18]. Then also, the system will verify the ID and address. If all are matched with the design, then data will exchange.

Device to the device authentication process, all blockchain centers broadcast all the aundro addresses. The IoT devices pass the information to the blockchain center and the community members to the advised information [19]. The IoT device follows a communication path, neat by community members or processes/collects data through the blockchain centers.

2.4. Alarm trigged phase

The two different coding schemes will trigger the alarm. i.e., local and global versions applied to hierarchical clustering.

Encoding and decoding:

First, introduce the encoding and decoding with the local version applied to hierarchal clustering. In this system, we should get the data structure by a searching agent [20]. Data structure decoding in binary form, shown in the figure 4, we can find the location by the binary encoded in the hierarchical tree shown in the figure 5.

2.3. Notification Phase

The figure 5 shows that the IoT blockchain platform structure contains many IoT device data storing sets. Community members, linked with one to one around the blockchain centers to provide a large amount of data by the community member, commands needed to perform some operations like enquire data, storing the data in the storage through the blockchain centers.

Data can be stored in the blockchain's physical device or the cloud. The community member anytime can access the data through the registered account [21]. Nowadays, embedded devices or android devices directly work as the transfer application interface. Finally, the data is directly communicated with the community member during the notification phase [22]. Figure 6 shows the IoT security guard system and Figure 7 shows the IoT Block chain platform.

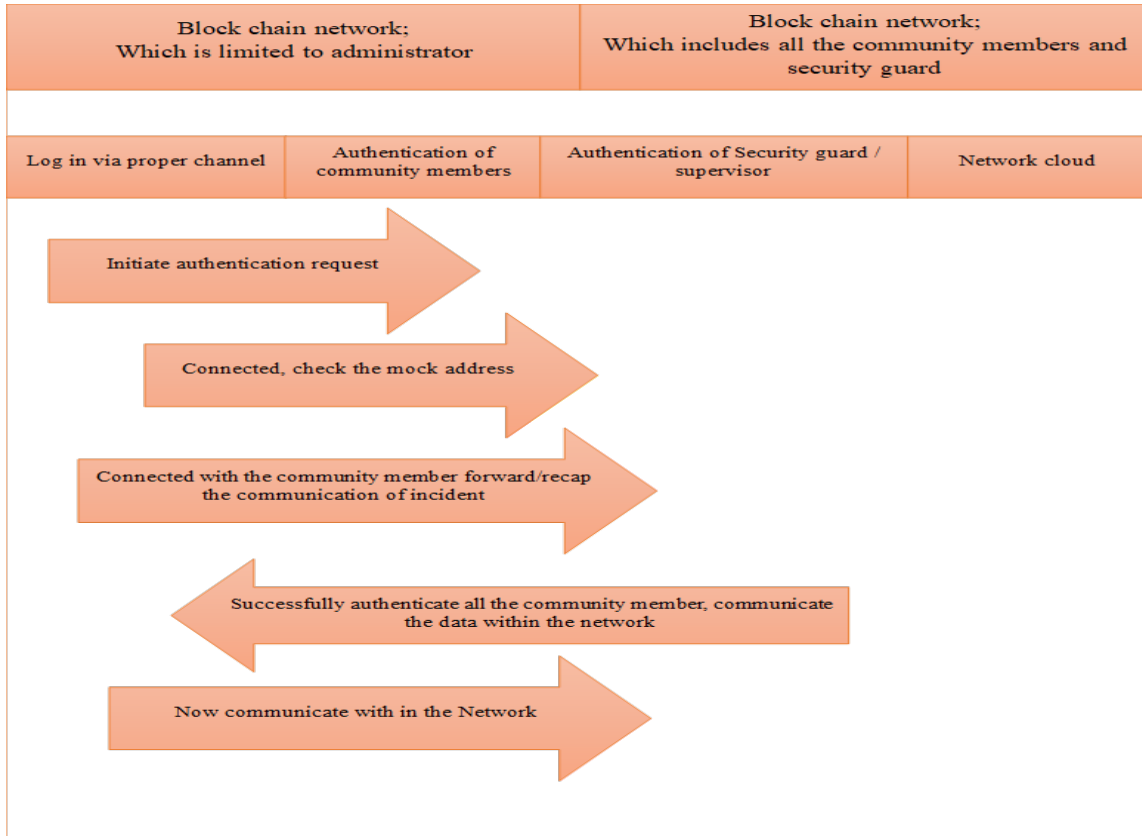


Figure 3. Authentication flow chart



(A) Coding scheme of the cluster



(B) Cluster center

Figure 4: Data structure decoding- Cluster center

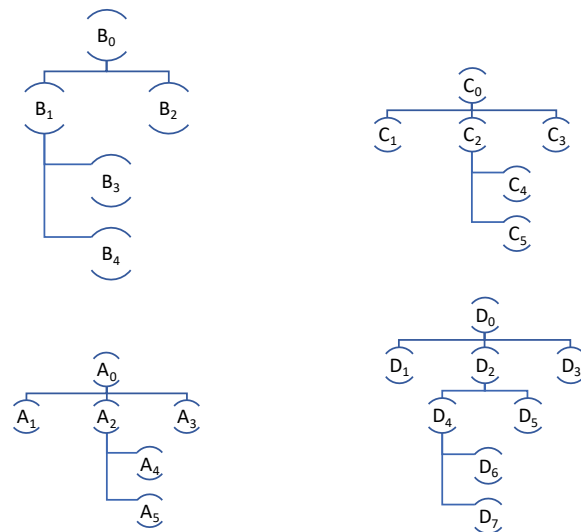


Figure 5: Hierarchical tree structure

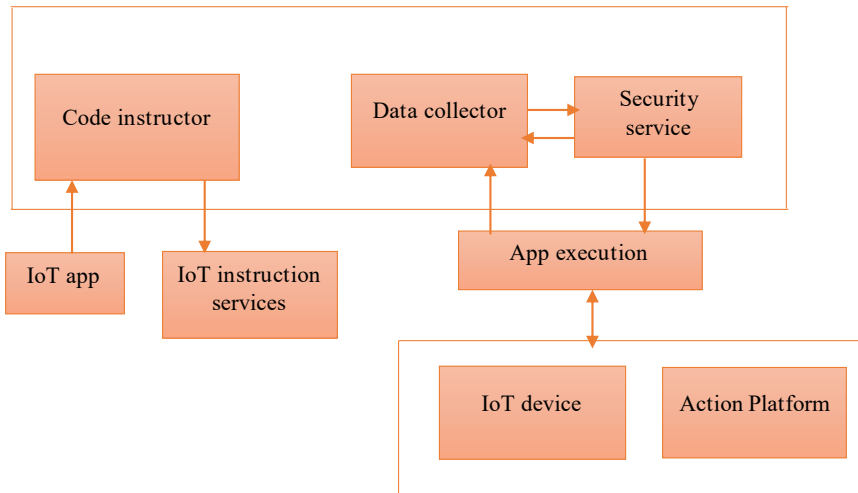


Figure 6: IoT security guard system

2.6. Response phase- Security guard with public domain IoT

IoT security guard is a dynamic controller, and it should work with good policy, which will protect the hazardous activities inside the community [23]. As per research work, IoT security guards act as a mediator between IoT devices and society. A developed system in blockchain centers; this center should be closed source, and it should not be cloud because it removes the need to believe the cloud providers.

IoT security guard verifies all events/actions inside the community; if any event/ action is against the policies, the security guard should respond [24]. IoT security guards need some part 1. Code instructor unit 2. data collecting processing unit 3. security server unit

Code instructor unit, instruct code as per security policies to the security guard. Code instructors always need updates like user instruction status and configuration settings.

The data collecting unit stores the information from the IoT devices/ collected data behavior observed so far; the data collector should work as an interface between IoT devices [25]. The data should be checked and responded to within a specified run time as per the community's policy.

The security guard services will provide two types of outputs. 1. Security guards should instruct every predicted condition, according to that need to take some actions [26]. If that action fails, then we need to pass the policy. 2. security guards work like an interface for accepting the policy by promoting the run time.

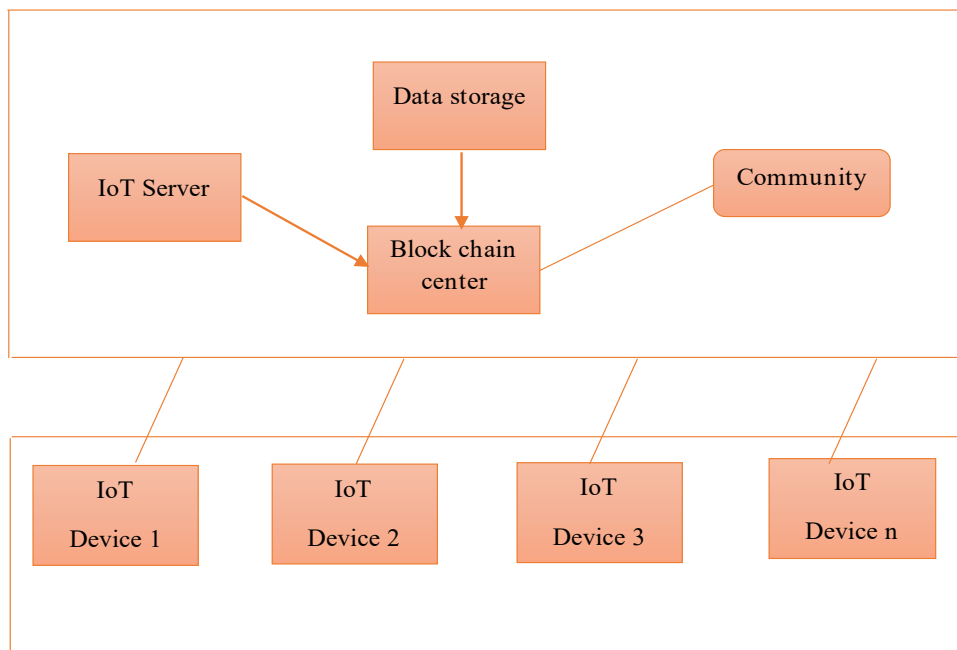


Figure 7: IoT Block chain platform

2.4. Check for history record phase

The system having two history records i.e.: stored/ recorded videos developed by IoT devices history records are stored by physical or cloud domain. Figure 8 shows the authentication to watch the videos and records.

step 1: Community member need to request to view the stored/ recorded videos and recodes of the private space through the security guard.

step 2: Security guard will wither requested data (i.e.: starting and ending date/ time and domain of his request). Then forwarded blockchain center release the data to security again he will check data.

step 3: Blockchain center will check the community member registered ID and address and permitted to security guard to release the information to the community member.

step 4: Security guard will release the information to the community member.

step 5: If block chain center could not verify/ community member is not in records then information should not permit to release.

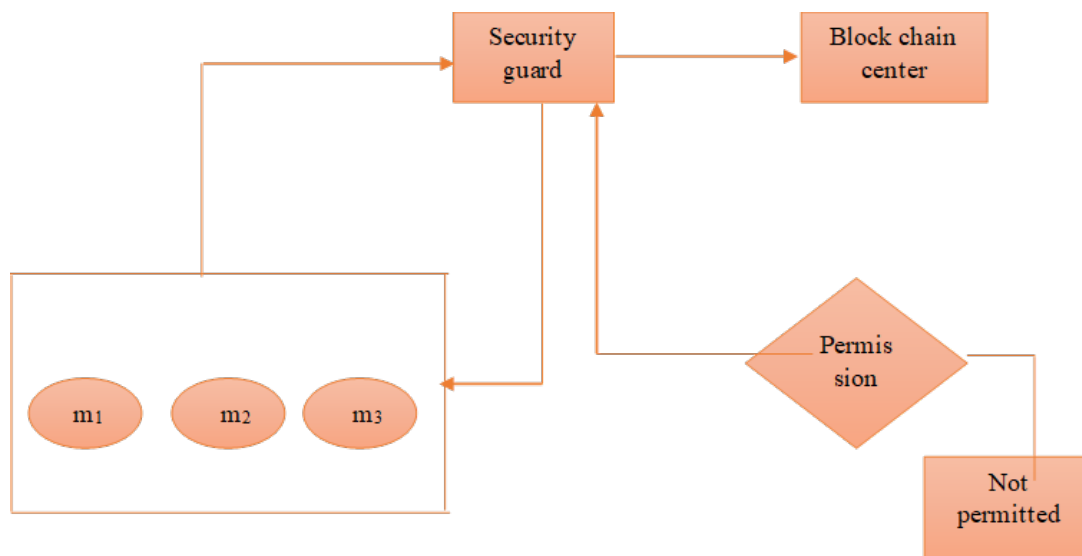


Figure 8: Authentication for viewing the information by community member

3. Analysis- Security

This work is essential because security analysis will present the attack. In this analysis, data integrity non-reputational message, unforgettable data, traceability of recorder, main-in-the-middle attack, reply attack.

3.1. Data Integrity

Blockchain is one of the most influential technologies to protect data. Blockchain stored the data in different boxes/storages. A chain connects these storages [27]. So due to this reason, hackers cannot hack the blockchain system is problematic because it needs more time to crack the different blocks/ storage and is also very costly.

It is essential to feature in blockchain any activity cannot perform without the notice of the security guard/admin. A very compact monitoring system is needed.

It is challenging to secure the data from IoT devices because IoT devices directly connect and transfer many data from the different connectors. But blockchain is supported is support the IoT device in the security purpose. Hear blockchain work like a protector of IoT devices.

Another problem with increasing innovative houses/communities. If we expand the smart homes/ community, we must also develop the blockchain algorithm. Due to this reason, data will protect safely. Table 1 below shows the summery of the attack on the smart things that have effected/

protected by something.

Table 1. Summary of the attack on the smart have effected/ protected by

Attack Name	Effect	effected/ protected by
Malicious block	Hackers Produce	Algorithm
Denial-Service	Unavailability of data	Admin/ Security Guard
Access control	Basic problem	Algorithm

3.2. Unforgeable data and Traceability:

In the developed system, hyper edger fabric-based blockchain technology is used, so it is stored in the blockchain center. In every step blockchain system is connected and updated from time to time [28]. When an IoT device is transferring or receiving data, the IoT device is triggered.

3.3. Man-in-the-middle attack:

In this developed system, a description for every command/communication/message defines every attack. Every message or communication/command is encrypted by the public key. After receiving the answer, the receiver can decode it by the private key to describe the communication.

4. Conclusion

This research is directly linked to the issues of safety in the community. To resolve the safety issue, developed a security system by integrating the blockchain and IoT devices. In our fundamental research, we create an architecture and flow of the work in multiple phases.

In this research, all the community members install the app with a blockchain system for feature communication. This communication will adequately transfer to the alarm for the ring as well, as the respective community member and relative community member can report through the log server record, and the community will notice the unsafe situations. During the entire communication process, all the updates will transfer/received by the community with the security.

This work is divided into many phases for managing personal and public IoT devices. Any community member can check these history records from their installed application as the security guard and admin permitted. In all the cases, the developed system can raise the community members' security from the third-party/hackers. The blockchain center will identify the hazardous activity if hackers try to hack the blockchain.

References

- [1]. Atlam, Hany & Alenezi, Ahmed & Alassafi, Madini & Wills, Gary. (2018). Blockchain with Internet of Things: Benefits, Challenges and Future Directions. *International Journal of Intelligent Systems and Applications*. 10. 10.5815/ijisa.2018.06.05.
- [2]. Alkhateeb, A.; Catal, C.; Kar, G.; Mishra, A. Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review. *Sensors* 2022, 22, 1304.
- [3]. Elva Leka and Besnik Selimi, "Development and Evaluation of Blockchain based Secure Application for Verification and Validation of Academic Certificates", *Annals of Emerging Technologies in Computing (AETiC)*, Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 22-36, Vol. 5, No. 2, 1st April 2021, Published by International Association of Educators and Researchers, (IAER), DOI: 10.33166/AETiC.2021.02.003, Available: <http://aetic.theiaer.org/archive/v5/v5n2/p3.html>
- [4]. Ana Reyna, Cristian Martín, Jaime Chen, Enrique Soler, Manuel Díaz, On blockchain and its integration with IoT. Challenges and opportunities, *Future Generation Computer Systems*, Volume 88, 2018, Pages 173-190, ISSN 0167-739X, <https://doi.org/10.1016/j.future.2018.05.046>.
- [5]. r nab Banerjee, Chapter Nine - Blockchain with IOT: Applications and use cases for a new

- paradigm of supply chain driving efficiency and cost, Editor(s): Shiho Kim, Ganesh Chandra Deka, Peng Zhang, *Advances in Computers*, Elsevier, Volume 115, 2019, Pages 259-292, ISSN 0065-2458, ISBN 9780128171899, <https://doi.org/10.1016/bs.adcom.2019.07.007>.
- [6]. Chen, C.-L.; Lim, Z.-Y.; Liao, H.-C. Blockchain-Based Community Safety Security System with IoT Secure Devices. *Sustainability* 2021, 13, 13994. <https://doi.org/10.3390/su132413994>
 - [7]. Panarello A, Tapas N, Merlino G, Longo F, Puliafito A. Blockchain and IoT Integration: A Systematic Survey. *Sensors (Basel)*. 2018 Aug 6;18(8):2575. doi: 10.3390/s18082575. PMID: 30082633; PMCID: PMC6111515.
 - [8]. Singh S, Ra I-H, Meng W, Kaur M, Cho GH. SH-BlockCC: A secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology. *International Journal of Distributed Sensor Networks*. April 2019. doi:10.1177/1550147719844159
 - [9]. Exploring the Integration of Blockchain Technology and IoT in a Smart University Application Architecture. (n.d.). Exploring the Integration of Blockchain Technology and IoT in a Smart University Application Architecture; dl.acm.org. Retrieved July 4, 2022, from <https://dl.acm.org/doi/fullHtml/10.1145/3459104.3459153>
 - [10]. Hasan, R. T. H. (2021, 0 0). Security Enhancement of IoT and Fog Computing Via Blockchain Applications. *JOURNAL OF SOFT COMPUTING AND DATA MINING*; www.google.com. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj9_5j57N_4AhXN1jgGHcQeBP44HhAWegQIBBAB&url=https%3A%2F%2Fpublisher.uthm.edu.my%2Fojs%2Findex.php%2Fjscdm%2Farticle%2Fdownload%2F8943%2F4557%2F&usq=AOvVaw3HB2ZFN0wVp2LI5M1IVKGi
 - [11]. Shivlal Mewada, Anil Saroliya, N. Chandramouli, T. Rajasanthosh Kumar, M. Lakshmi, S. Suma Christal Mary, Mani Jayakumar, "Smart Diagnostic Expert System for Defect in Forging Process by Using Machine Learning Process", *Journal of Nanomaterials*, vol. 2022, Article ID 2567194, 8 pages, 2022. <https://doi.org/10.1155/2022/2567194>
 - [12]. Shivlal Mewada, Anil Saroliya, N. Chandramouli, T. Rajasanthosh Kumar, M. Lakshmi, S. Suma Christal Mary, Mani Jayakumar, "Smart Diagnostic Expert System for Defect in Forging Process by Using Machine Learning Process", *Journal of Nanomaterials*, vol. 2022, Article ID 2567194, 8 pages, 2022. <https://doi.org/10.1155/2022/2567194>
 - [13]. Li, W., Wu, J., Cao, J. et al. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *J Cloud Comp* 10, 35 (2021). <https://doi.org/10.1186/s13677-021-00247-5>
 - [14]. Shobanadevi, A., Tharewal, S., Soni, M. et al. Novel identity management system using smart blockchain technology. *Int J Syst Assur Eng Manag* (2021). <https://doi.org/10.1007/s13198-021-01494-0>
 - [15]. M. Soni and D. K. Singh, "Blockchain Implementation for Privacy preserving and securing the Healthcare data," 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), 2021, pp. 729-734, doi: 10.1109/CSNT51715.2021.9509722.
 - [16]. Soni, M., & Singh, D. K. (2023). A key exchange system for secure data coordination in healthcare systems. In *Healthcare Analytics (Vol. 3, p. 100138)*. Elsevier BV. <https://doi.org/10.1016/j.health.2023.100138>
 - [17]. Jagota, V., Luthra, M., Bhola, J., Sharma, A., & Shabaz, M. (2022). A Secure Energy-Aware Game Theory (SEGaT) Mechanism for Coordination in WSAWs. In *International Journal of Swarm Intelligence Research (Vol. 13, Issue 2, pp. 1–16)*. IGI Global. <https://doi.org/10.4018/ijisir.287549>
 - [18]. Huaqun Guo, Xingjie Yu, A survey on blockchain technology and its security, *Blockchain: Research and Applications*, Volume 3, Issue 2, 2022, 100067, ISSN 2096-7209, <https://doi.org/10.1016/j.bcra.2022.100067>.
 - [19]. Yao, Q., Shabaz, M., Lohani, T. K., Wasim Bhatt, M., Panesar, G. S., & Singh, R. K. (2021). 3D modelling and visualization for Vision-based Vibration Signal Processing and Measurement. In *Journal of Intelligent Systems (Vol. 30, Issue 1, pp. 541–553)*. Walter de Gruyter GmbH. <https://doi.org/10.1515/jisys-2020-0123>
 - [20]. Li, Xiaoqi & Jiang, Peng & Chen, Ting & Luo, Xiapu & Wen, Qiaoyan. (2017). A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*. 107. 10.1016/j.future.2017.08.020.
 - [21]. Zhang, X., Rane, K. P., Kakaravada, I., & Shabaz, M. (2021). Research on vibration

- monitoring and fault diagnosis of rotating machinery based on internet of things technology. In *Nonlinear Engineering* (Vol. 10, Issue 1, pp. 245–254). Walter de Gruyter GmbH. <https://doi.org/10.1515/nleng-2021-0019>
- [22]. Samuel, O.; Almogren, A.; Javaid, A.; Zuair, M.; Ullah, I.; Javaid, N. Leveraging Blockchain Technology for Secure Energy Trading and Least-Cost Evaluation of Decentralized Contributions to Electrification in Sub-Saharan Africa. *Entropy* 2020, 22, 226. <https://doi.org/10.3390/e22020226>
- [23]. K. Meenakshi and K. Sashi Rekha, "An enhanced security system using blockchain technology for strong fmc relationship," *Intelligent Automation & Soft Computing*, vol. 35, no.1, pp. 111–128, 2023.
- [24]. Soni, M., & Singh, D. K. (2022). Privacy-preserving secure and low-cost medical data communication scheme for smart healthcare. In *Computer Communications* (Vol. 194, pp. 292–300). Elsevier BV. <https://doi.org/10.1016/j.comcom.2022.07.046>
- [25]. Chen, Z., Cong, B., Hua, Z., Cengiz, K., & Shabaz, M. (2021). Application of clustering algorithm in complex landscape farmland synthetic aperture radar image segmentation. In *Journal of Intelligent Systems* (Vol. 30, Issue 1, pp. 1014–1025). Walter de Gruyter GmbH. <https://doi.org/10.1515/jisys-2021-0096>
- [26]. Kurnia, R.I., Girsang, A.S., "Classification of user comment using word2vec and deep learning", (2021) *International Journal of Emerging Technology and Advanced Engineering*, 11 (5), pp. 1-8. DOI: 10.46338/IJETAE0521_01
- [27]. Liu, Y., & Shabaz, M. (2021). Design and research of computer network micro-course management system based on JSP technology. In *International Journal of System Assurance Engineering and Management*. Springer Science and Business Media LLC. <https://doi.org/10.1007/s13198-021-01368-5>
- [28]. Fayaz, S. A. ., Zaman, M. ., & Butt, M. A. . (2022). Numerical and Experimental Investigation of Meteorological Data Using Adaptive Linear M5 Model Tree for the Prediction of Rainfall . *Review of Computer Engineering Research*, 9(1), 1–12. <https://doi.org/10.18488/76.v9i1.2961>.